UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JILL KINNEY, individually and on behalf of all others similarly situated, Plaintiff, v. ANNA JAQUES HOSPITAL and BETH ISRAEL LAHEY HEALTH, INC., Defendants.	Case No. _____ CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Jill Kinney ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendants Anna Jaques Hospital ("AJH") and Beth Israel Lahey Health, Inc. ("BILH" and, with AJH, "Defendants"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard approximately 316,342 persons' (including Plaintiff's) personally identifying information ("PII") and personal health information ("PHI"), including names, demographic information, medical information, health insurance information, Social Security numbers, driver's license numbers, financial information, and other personal or health information.

2. AJH is a hospital that offers services to the Merrimack Valley, North Shore, and Southern New Hampshire areas. BILH is a health care system that oversees several hospitals and other health care service providers across Massachusetts and New Hampshire.

3. On or about December 25, 2023, AJH discovered that an unauthorized third party had gained access to its network systems and accessed and acquired files containing the PII/PHI of BILH and AJH's patients, including Plaintiff and Class members (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which AJH discovered on or about December 25, 2023.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of the New Hampshire Consumer Protection Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Jill Kinney

7. Plaintiff Jill Kinney is a citizen of New Hampshire.

8. Plaintiff Kinney received healthcare or related services from Defendants at Anna Jaques Hospital. As a condition of providing healthcare or related services to Plaintiff Kinney, Defendants required Plaintiff Kinney to provide them with her PII/PHI.

9. Based on representations made by Defendants, Plaintiff Kinney believed Defendants had implemented and maintained reasonable security and practices to protect her PII/PHI. With this belief in mind, Plaintiff Kinney provided her PII/PHI to Defendants in connection with obtaining healthcare or related services provided by Defendants.

10. At all relevant times, AJH stored and maintained Plaintiff Kinney's PII/PHI on its network systems.

11. Plaintiff Kinney received a letter from AJH notifying her that her PII/PHI was in the files accessed in the Data Breach.

12. Had Plaintiff Kinney known that Defendants do not adequately protect the PII/PHI they collect and maintain, she would not have agreed to provide Defendants with her PII/PHI or obtained healthcare or related services from Defendants.

13. Plaintiff Kinney experienced identity theft as a result of the Data Breach. In or about November, 2023, Plaintiff Kinney experienced fraudulent charges on her credit card as a result of the Data Breach. Plaintiff Kinney spent time and effort contacting her credit card company to address the fraudulent charges.

14. As a direct result of the Data Breach, Plaintiff Kinney has suffered other injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of her highly sensitive PII/PHI; and deprivation of the value of her PII/PHI.

Defendant Anna Jaques Hospital

15. Defendant Anna Jaques Hospital is a Massachusetts nonprofit corporation with its principal place of business located at 25 Highland Ave., Newburyport, MA 01950.

Defendant Beth Israel Lahey Health, Inc.

16. Defendant Beth Israel Lahey Health, Inc. is a Massachusetts nonprofit corporation with its principal place of business located at 20 University Rd., Suite 700, Cambridge, MA 02138.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

18. This Court has general personal jurisdiction over both Anna Jaques Hospital and Beth Israel Lahey Health, Inc., because they are Massachusetts corporations and maintain their principal places of business in Massachusetts.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants' principal places of business are in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

20. AJH is an 83-bed "not-for-profit community hospital serving the Merrimack Valley, North Shore and Southern New Hampshire areas."[1] BILH is a healthcare system

[1] *About Anna Jaques Hospital*, ANNA JAQUES HOSP., https://ajh.org/about (last accessed Dec. 13, 2024).

comprising "academic medical centers and teaching hospitals, specialty and community hospitals, more than 4,700 physicians and 39,000 employees."[2] AJH is part of Beth Israel Lahey Health.[3]

21. In the regular course of their business, Defendants collect and maintain the PII/PHI of their current and former patients, including Plaintiff and Class members. Defendants required Plaintiff and Class members to provide their PII/PHI to AJH as a condition of providing healthcare or related services.

22. BILH's website contains a Notice of Privacy Practices (the "Privacy Policy") that describes the way BILH and its covered entities, including AJH, may use and disclose PII/PHI.[4] AJH's website also contains the identical Privacy Policy.[5]

23. Defendants state in the Privacy Policy that they will use PII/PHI for specified purposes, including for treatment, payment, and health care operations.[6]

24. In the Privacy Policy, Defendants admit they are required by law to, among other things, "make sure medical information that identifies you is kept private," "notify you if there is a breach of your unsecured personal health information," and "follow the terms of the [Privacy Policy]."[7]

25. Defendants promise in the Privacy Policy that "uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission."[8]

---

[2] *About Beth Israel Lahey Health*, BILH, https://bilh.org/about (last accessed Dec. 13, 2024).
[3] *About Anna Jaques Hospital*, *supra* note 1.
[4] *Notice of Privacy Practices*, BILH (May 2022), https://bilh.org/-/media/files/bilh/bilh-privacy-practices-notice-2022.pdf [hereinafter, the "*Privacy Policy*"].
[5] *Notice of Privacy Practices*, AJH (May 2022), https://ajh.org/-/media/files/bilh/bilh-privacy-practices-notice-2022.pdf.
[6] *Privacy Policy*, *supra* note 4.
[7] *Id.*
[8] *Id.*

26. Defendants acknowledge that once they have disclosed PII/PHI, that disclosure cannot be undone.[9]

27. AJH promises its patients that it will "[r]espect your privacy."[10] AJH tells its patients they have a right to "[p]rivacy and confidentiality."[11]

28. Plaintiff and Class members are current and former patients of Defendants who shared their PII/PHI with Defendants.

The Data Breach

29. On or about December 25, 2023, AJH discovered that an unauthorized third party had gained access to its network systems and accessed and acquired files containing the PII/PHI of Plaintiff and Class members.[12] AJH's investigation revealed that the cybercriminals responsible for the Data Breach accessed and removed files containing the PII/PHI of Plaintiff and Class members, including their name, "demographic information, medical information, health insurance information, Social Security number, driver's license number, financial information, and other personal or health information."[13]

30. On January 19, 2024, the Money Message ransomware group claimed responsibility for the attack on AJH.[14] The Money Message ransomware group utilizes a "double

[9] *Id.*
[10] *Patient Rights & Responsibilities*, ANNA JAQUES HOSP., https://ajh.org/patients-visitors/rights-responsibilities (last accessed Dec. 13, 2024).
[11] *Id.*
[12] *Anna Jaques Notice Regarding Data Security Incident*, ANNA JAQUES HOSP. (Dec. 5, 2024), https://ajh.org/-/media/files/ajh/ajh-data-security-incident-notice.pdf.
[13] *Id.*
[14] Steve Alder, *Anna Jacques Hospital Notifies 316K Patients About December 2023 Ransomware Attack*, HIPAA J. (Dec. 9, 2024), https://www.hipaajournal.com/anna-jacques-hospital-december-2023-ransomware-attack/.

extortion" technique when targeting a company.[15] In double extortion ransomware attacks, the cybercriminals "exfiltrate a victim's sensitive data in addition to encrypting it," which makes this type of attack "especially dangerous."[16]The Money Message ransomware group claimed to have stolen 600 GB of data from AJH's network systems, and listed AJH on its dark web data leak website, along with screenshots of some of the stolen information.[17] The group also claimed to have data related to BILH.[18]

31. On January 26, 2024, the Money Message ransomware group published the entirety of the PII/PHI stolen from Defendants on their dark web site.[19] That stolen PII/PHI is still on Money Message's dark web site, "where it has remained available for anyone to download for 11 months and counting."[20] "Given that the Money Message ransomware group that attacked it leaked all the data it stole in January 2024," cybercriminals, identity thieves, and fraudsters have "had plenty of time to monetize it."[21]

---

[15] *The Money Message Group - A New Ransomware Threat*, AVERTIUM (May 23, 2023), https://www.avertium.com/resources/threat-reports/the-money-message-group-a-new-ransomware-threat.

[16] *What Is Double Extortion Ransomware?*, ZSCALER, https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware (last accessed Dec. 13, 2024).

[17] Alder, *supra* note 14.

[18] Jonathan Greig, *Ransomware gang claims responsibility for Christmas attack on Massachusetts hospital*, THE RECORD (Jan. 19, 2024), https://therecord.media/ransomware-gang-claims-responsibility-hospital-christmas-attack.

[19] *E.g.*, Alder, *supra* note 14; Pierluigi Paganini, *2023 Anna Jaques Hospital data breach impacted over 310,000 people*, SEC. AFF. (Dec. 9, 2024), https://securityaffairs.com/171801/data-breach/anna-jaques-hospital-data-breach.html.

[20] Alder, *supra* note 14; *see also* Marianne Kolbasuk McGee, *Hospital Notifies 316,000 of Breach in Christmas 2023 Hack*, GOV'T INFO. SEC. (Dec. 10, 2024), https://www.govinfosecurity.com/hospital-notifies-316000-breach-in-christmas-2023-hack-a-27016.

[21] Phil Muncaster, *Anna Jacques Hospital Ransomware Breach Hits 316K Patients*, INFOSEC. MAG. (Dec. 9, 2024), https://www.infosecurity-magazine.com/news/anna-jacques-hospital-ransomware/.

32. Once PII/PHI like that compromised in the Data Breach is published on the dark web, "you'll be more vulnerable to identity theft and online scams."[22] When PII/PHI is available on the dark web, "cybercriminals can easily access it to create personalized phishing attacks -- or worse, steal your identity."[23] Signs that a person's PII/PHI is available on the dark web and is being misused include, among other things, spam calls, emails, or messages, and unfamiliar purchases on credit cards.[24] PII/PHI exposed in the Data Breach can also be combined with other information about victims of the Data Breach, resulting in additional risk; as this information "pools together, hackers use it to fuel other criminal operations, combining details and reusing them for subsequent attacks."[25]

33. Additionally, the Data Breach and the attack by the Money Message ransomware group disrupted the electronic health records system at AJH, resulting in AJH turning away ambulances until it restored its compromised systems.[26]

34. While AJH learned of the Data Breach on or about December 25, 2023, and learned the Money Message ransomware group took credit for the attack and was threatening to publish the stolen PII/PHI on or about January 19, 2024, Defendants waited until approximately December 5, 2024, nearly a full year later, to begin notifying its patients affected in the Data Breach that their PII/PHI had been compromised. And while Defendants waited a year to notify patients that they

---

[22] Geoff Williams, *Is Your Private Data on the Dark Web? Experts Share the Warning Signs and Tips Protect Yourself*, CNET (Nov. 18, 2024 11:00 AM), https://www.cnet.com/personal-finance/is-your-private-data-on-the-dark-web-experts-share-the-warning-signs-and-tips-protect-yourself/.
[23] *Id.*
[24] *Id.*
[25] *What is the Dark Web? And Is Your Personal Info There?*, BITEDEFENDER, https://www.bitdefender.com/en-us/cyberpedia/what-is-dark-web (last accessed Dec. 13, 2024).
[26] *E.g.*, Joe Warminsky, *Cyberattack on Massachusetts hospital disrupted records system, emergency services*, THE RECORD (Dec. 29, 2023), https://therecord.media/cyberattack-on-massachusetts-hospital-disrupted-health-record-system.

were affected in the Data Breach, it still has not notified patients that their PII/PHI was published on the dark web by the cybercriminals responsible for the Data Breach, or that their PII/PHI has been freely available to cybercriminals for 11 months.

35. Defendants' failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen, or that it was published on the dark web, virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendants Knew that Criminals Target PII/PHI

36. At all relevant times, Defendants knew, or should have known, that the PII/PHI that they collected and maintain was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks that it should have anticipated and guarded against.

37. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[27]

[27] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

38. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2024 report, the healthcare compliance company Protenus found that there were 1,161 medical data breaches in 2023 with over 171 million patient records exposed.[28] This is an increase from the 1,138 medical data breaches which exposed approximately 59 million records that Protenus compiled in 2023.[29]

39. PII/PHI is a valuable property right.[30] The value of PII/PHI as a commodity is measurable.[31] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[32] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[33] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

40. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and

[28] *See 2024 Breach Barometer*, PROTENUS 2, https://protenus.com/hubfs/Breach_Barometer/Latest%20Version/Protenus%20-%20Industry%20Report%20-%20Privacy%20-%20Breach%20Barometer%20-%202024.pdf (last accessed Dec. 13, 2024).
[29] *See id*.
[30] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[31] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.
[32] Organization for Economic Co-operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[33] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

41. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[34] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[35]

42. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security Numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[36] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[37]

43. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[38] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and

---

[34] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[35] *Id.*
[36] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[37] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[38] Steager, *supra* note 34.

extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[39]

44. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[40]

45. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

46. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[41] [42]

---

[39] *Id.*

[40] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[41] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Dec. 13, 2024).

[42] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

47. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[43]

48. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[44]

49. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[45] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[46] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [47] The FTC also warns, "If the thief's health information is mixed with yours it

---

[43] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[44] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Dec. 13, 2024).

[45] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

[46] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 37.

[47] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Dec. 13, 2024).

could affect the medical care you're able to get or the health insurance benefits you're able to use."[48]

50. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

b. Significant bills for medical goods and services neither sought nor received.

c. Issues with insurance, co-pays, and insurance caps.

d. Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

e. Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

f. As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

g. Phantom medical debt collection based on medical billing or other identity information.

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [49]

51. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

[48] *Id.*
[49] *See* Dixon & Emerson, *supra* note 45.

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[50]

52. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

53. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, theft, and publication of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

54. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

55. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

[50] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

> All persons whose personally identifiable information and personal health information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

56. Excluded from the Class are Anna Jaques Hospital, and its affiliates, parents, subsidiaries, officers, agents, and directors; Beth Israel Lahey Health, Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors; as well as the judge(s) presiding over this matter and the clerks of said judge(s).

57. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. AJH has reported to the Office of the Maine Attorney General that the Data Breach affected 316,342 persons.[51]

59. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendants had a duty not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

[51] *Anna Jaques Hospital*, ME. ATT'Y GEN. OFF. (Dec. 5, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ecfcfbba-9bcf-4909-ab3b-2cd996e79cfa.html.

e. Whether Defendants breached their duties to protect Plaintiff's and Class members' PII/PHI; and

f. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

60. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

61. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

62. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

63. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

64. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

65. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

66. Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

67. Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII/PHI.

68. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure

systems. Defendants knew, or should have known, of the many data breaches that targeted companies that collect and store PII/PHI in recent years.

69. Given the nature of Defendants' business, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

70. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to them—including Plaintiff's and Class members' PII/PHI.

71. Plaintiff and Class members had no ability to protect their PII/PHI that was, or remains, in Defendants' possession.

72. It was or should have been reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

73. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised. The PII/PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendants'

failure to exercise reasonable care in safeguarding, securing, and protecting such PII/PHI by, *inter alia*, adopting, implementing, and maintaining appropriate security measures.

74. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF FIDUCIARY DUTY

75. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

76. As a condition of obtaining services from Defendants, Plaintiff and Class members gave Defendants their PII/PHI in confidence, believing that Defendants would protect that information. Plaintiff and Class members would not have provided Defendants with this information had they known it would not be adequately protected. Defendants' acceptance, use, and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Defendants and Plaintiff and Class members. In light of this relationship, Defendants

must act primarily for the benefit of their patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

77. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. They breached that duty by, among other things, failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that they collected, utilized, and maintained.

78. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

79. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

80. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Defendants.

81. Pursuant to these implied contracts, Plaintiff and Class members paid money to Defendants (directly or through their insurance) and provided Defendants with their PII/PHI. In exchange, Defendants agreed to, among other things, and Plaintiff and Class members and Defendants mutually understood that Defendants would: (1) provide healthcare or related services to Plaintiff and Class members; (2) use Plaintiff's and Class members' PII/PHI to facilitate providing healthcare services to Plaintiff and Class members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (4) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations, industry standards, and Defendants' representations regarding their security and privacy practices

82. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Defendants, on the other hand. Indeed, as set forth *supra*, Defendants recognized the importance of data security and the privacy of their patients' PII/PHI on their respective websites. Plaintiff and Class members and Defendants mutually understood and agreed that the healthcare or related services Defendants would provide to Plaintiff and Class members included Defendants' protection of Plaintiff's and Class members' privacy and PII/PHI. Had Plaintiff and Class members known that Defendants would not adequately protect their patients' and former patients' PII/PHI, they would not have paid for or obtained healthcare or related services from Defendants.

83. Plaintiff and Class members performed their obligations under the implied contract when they provided Defendants with their PII/PHI and paid for healthcare or related services from Defendants, expecting that their PII/PHI would be protected.

84. Defendants breached their obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

85. Defendants' breach of their obligations of the implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the resulting injuries to Plaintiff and Class members.

86. Plaintiff and all other Class members were damaged by Defendants' breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they now face a substantially increased and imminent risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) they overpaid for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

87. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

88. This claim is pleaded in the alternative to the breach of implied contract claim.

89. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of monies paid for healthcare or related services, with an implicit understanding that Defendants would use some of these payments to protect the PII/PHI they collect, store, and use to provide health care.

90. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members. Defendants also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate billing and payment services and other aspects of Defendants' business.

91. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

92. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

93. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

COUNT V
VIOLATIONS OF THE NEW HAMPSHIRE CONSUMER PROTECTION ACT ("NHCPA")
N.H. Rev. Stat. § 358

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. Defendants, Plaintiff, and Class members are all "persons" as defined in the NHCPA. N.H. Rev. Stat. § 358-A:1(I).

96. Defendants' healthcare services are "trade" and "commerce" as defined in the NHCPA. N.H. Rev. Stat. § 358-A:1(II).

97. The NCHPA states, "It shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state." N.H. Rev. Stat. § 358-A:2.

98. The NHCPA provides a list of the unfair methods of competition or unfair or deceptive practices under the act. *Id*. Defendants' failure to adequately protect Plaintiff's and Class members' PII/PHI while making representations to Plaintiff and Class members that their PII/PHI would be protected or omitting that Defendants would fail to adequately protect Plaintiff's and Class members' PII/PHI is an unfair method of competition or unfair or deceptive practice under at least the following categories defined in the NHCPA:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that such person does not have. N.H. Rev. Stat. § 358-A:2(V).

b. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another. N.H. Rev. Stat. § 358-A:2(VII).

c. Advertising goods or services with intent not to sell them as advertised. N.H. Rev. Stat. § 358-A:2(IX).

99. Had Plaintiff and Class members known that Defendants would not adequately protect their PII/PHI, Plaintiff and Class members would not have sought services from Defendants.

100. As a result of Defendants' misrepresentations, omissions, and unfair conduct, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

101. Plaintiff seeks actual damages, individually and on behalf of the Class, pursuant to N.H. Rev. Stat. § 358-A:10 and A:10-a. Plaintiff also seeks injunctive or other equitable relief and reasonable attorney's fees. *Id*.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against Defendants as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 13, 2024

Respectfully submitted,

/s/ *David Pastor*

David Pastor (BBO 391000)
PASTOR LAW OFFICE PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Tel: 617-742-9700
Fax: 617-742-9701
dpastor@pastorlawoffice.com

Ben Barnow*
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
Cook County Attorney No. 38957
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff Jill Kinney

**Pro hac vice* forthcoming